Multiplicative Character Sums of Fermat Quotients and Pseudorandom Sequences

Domingo Gomez
University of Cantabria,
Avd. de los Castros, s/n, Santander, Spain
domingo.gomez@unican.es

Arne Winterhof
Johann Radon Institute for
Computational and Applied Mathematics,
Austrian Academy of Sciences,
Altenberger Straße 69, A-4040 Linz, Austria
arne.winterhof@oeaw.ac.at

July 16, 2012

Abstract

We prove a bound on sums of products of multiplicative characters of shifted Fermat quotients modulo p. From this bound we derive results on the pseudorandomness of sequences of modular discrete logarithms of Fermat quotients modulo p: bounds on the well-distribution measure, the correlation measure of order ℓ, and the linear complexity.

MSC: Primary 11T24 Secondary 11K45 11K36 11T71 94A55

Keywords: Fermat quotients, finite fields, character sums, pseudorandom sequences, discrete logarithm, correlation measure, linear complexity.

1 Introduction

For a prime p and an integer u with $\gcd(u,p)=1$ the *Fermat quotient* $q_p(u)$ *modulo* p is defined as the unique integer with

$$q_p(u) \equiv \frac{u^{p-1}-1}{p} \pmod p, \qquad 0 \le q_p(u) \le p-1,$$

and we define $q_p(u) = 0$ if $u \equiv 0 \bmod p$. There are several results which involve the distribution and structure of Fermat quotients $q_p(u)$ modulo p and they have numerous applications in computational and algebraic number theory, see e.g. [1, 3, 5, 6, 7, 8, 13, 15] and references therein. In particular, Shparlinski [15] proved a bound on character sums for any nontrivial multiplicative character ψ, which can be easily extended to,

$$\sum_{u=0}^{N-1} \psi(q_p(au+b)) \ll N^{1-1/\nu} p^{(5\nu+1)/(4\nu^2)} (\log p)^{1/\nu}, \ 1 \le N \le p^2, \quad (1)$$

for any integers a, b with $\gcd(a, p^2) \ne p^2$, where $U \ll V$ is equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$ which depends only on the parameter ν or is absolute otherwise. Here we study the following multiplicative character sums,

$$\sum_{u=0}^{N-1} \psi_1(q_p(u+d_1)) \cdots \psi_\ell(q_p(u+d_\ell)), \quad 1 \le N \le p^2,$$

with nontrivial multiplicative characters $\psi_1, \ldots, \psi_\ell$ modulo p and lags $0 \le d_1 < d_2 < \ldots < d_\ell \le p^2 - 1$. We prove a bound on these character sums of order of magnitude

$$\max\left\{\frac{\ell N}{p^{1/3}}, \ell p^{3/2} \log p\right\}$$

in Section 2. Besides standard arguments the proof is based on a result of Heath-Brown [8, Lemma 4] on the number of solutions of the congruences

$$\sum_{i=1}^{p-1} \frac{u^i}{i} \equiv c \bmod p, \quad 0 \le u \le p-1.$$

We apply this character sum bound to derive results on the pseudorandomness of sequences (e_u) of *discrete logarithms* modulo a divisor $m \ge 2$ of $p-1$ of Fermat quotients modulo p defined by

$$\exp(2\pi i e_u/m) = \chi(q_p(u)), \ 0 \le e_u < m \quad \text{if } q_p(u) \not\equiv 0 \bmod p \quad (2)$$

and $e_u = 0$ otherwise, where χ is a fixed multiplicative character modulo p of order m. We prove bounds on the *well-distribution measure*, *correlation measure of order* ℓ, and the Nth *linear complexity* of (e_u) in Section 3.

Acknowledgment

The authors wish to thank Alina Ostafe and Igor Shparlinski for motivating discussions.

2 The character sum bound

In this section we prove the following character sum bound.

Theorem 1 *Let $\psi_1, \ldots, \psi_\ell$ be nontrivial multiplicative characters modulo p. Then we have*

$$\sum_{u=0}^{N-1} \psi_1(q_p(u+d_1)) \cdots \psi_\ell(q_p(u+d_\ell)) \ll \max\left\{\frac{\ell N}{p^{1/3}}, \ell p^{3/2} \log p\right\}$$

for any integers $0 \le d_1 < \ldots < d_\ell \le p^2 - 1$ and $1 \le N \le p^2$.

Proof. For $\ell = 1$ the result follows from (1) and we may assume $\ell \ge 2$. We recall that for $\gcd(v, p) = 1$ we have

$$q_p(v + kp) \equiv q_p(v) - kv^{-1} \bmod p. \tag{3}$$

Substituting $u = v + kp$ with $0 \le v \le p - 1$ and put $K = \lfloor N/p \rfloor$ we get

$$\sum_{u=0}^{N-1} \psi_1(q_p(u+d_1)) \cdots \psi_\ell(q_p(u+d_\ell)) \ll \ell p \; + \sum_{\substack{v=0 \\ v+d_i \not\equiv 0 \bmod p,\ i=1,\ldots,\ell}}^{p-1} S_v,$$

where

$$S_v = \left| \sum_{k=0}^{K-1} \psi_1((q_p(v+d_1) - k(v+d_1)^{-1}) \cdots \psi_\ell(q_p(v+d_\ell) - k(v+d_\ell)^{-1})) \right|.$$

If $q_p(v+d_1)(v+d_1) \not\equiv q_p(v+d_j)(v+d_j) \bmod p$ for $j = 2, \ldots, \ell$, the standard method for reducing incomplete character sums to complete ones and the Weil-bound, see for example [9] or [14, Lemma 3.4], lead to the bound

$$S_v \ll \ell p^{1/2} \log p.$$

Otherwise we estimate S_v trivially by K.

To complete the proof it remains to show that for fixed $2 \le j \le \ell$ the number of $0 \le v \le p-1$ with

$$q_p(v+d_1)(v+d_1) \equiv q_p(v+d_j)(v+d_j) \bmod p \tag{4}$$

is of order of magnitude $p^{2/3}$. If $d_j \equiv d_1 \bmod p$ (but $d_j \not\equiv d_1 \bmod p^2$), (3) with $k = (d_j - d_1)/p$ implies $v + d_1 \equiv 0 \bmod p$. Hence, since additionally $q_p(v+d_1)(v+d_1) - q_p(v+d_2)(v+d_2)$ is p-periodic we may assume $d_1 = 0$ and $d_j = d$ with $1 \le d \le p-1$. Note that

$$q_p(dw) \equiv q_p(d) + q_p(w) \bmod p, \quad \gcd(dw, p) = 1.$$

Hence, substituting $v = d(w-1)$ in (4) (with $d_1 = 0$ and $d_j = d$) we get for $2 \le w \le p-1$,

$$\begin{aligned} c &\equiv q_p(dw)dw - q_p(d(w-1))d(w-1) \\ &\equiv q_p(w)dw - q_p(w-1)d(w-1) + q_p(d)d \bmod p, \end{aligned}$$

for some constant c. So, we can transform our problem into studying

$$\frac{(w-1)^p - w^p + 1}{p} \equiv q_p(d) - c \bmod p.$$

The left hand side is equal to

$$\frac{\sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} w^i}{p} \equiv \sum_{i=1}^{p-1} \frac{w^i}{i} \bmod p$$

and the number of solutions can be estimated by $\ll p^{2/3}$, see [8, Lemma 4]. $\square$

3 Measures of pseudorandomness

In this section we study three measures of pseudorandomness for the sequence (e_u) defined by (2). For a survey on pseudorandom sequences we refer to [16].

For $c \in \{0, 1, \ldots, m-1\}$ put

$$x((e_u), c, M, a, b) = |\{\ u : 0 \le u \le M-1,\ e_{au+b} = c\}|$$

and for $w = (a_1, \ldots, a_\ell) \in \{0, 1, \ldots, m-1\}^\ell$ and $D = (d_1, \ldots, d_\ell)$ with integers $0 \le d_1 < \ldots < d_\ell < p^2$

$$g((e_u), w, M, D) = |\{u : 0 \le u \le M-1, (e_{u+d_1}, \ldots, e_{u+d_\ell}) = w\}|.$$

Then the *f-well-distribution measure* of (e_u) ('f' for 'frequency') is defined as

$$\delta((e_u)) = \max_{c,M,a,b} \left| x((e_u), c, M, a, b) - \frac{M}{m} \right|,$$

where the maximum is taken over all $c \in \{0, 1, \ldots, m-1\}$ and a, b, M with $a + (M-1)b < p^2$, while the *f-correlation measure of order* ℓ is defined as

$$\gamma_\ell((e_u)) = \max_{w,M,D} \left| g((e_u), w, M, D) - \frac{M}{m^\ell} \right|,$$

where the maximum is taken over all $w \in \{0, 1, \ldots, m-1\}^\ell$, $D = (d_1, \ldots, d_\ell)$ and M such that $M + d_\ell \le p^2$. The f-well-distribution measure and the f-correlation measure of order ℓ were introduced in [11].

Theorem 2 *For the sequence* (e_u) *defined by* (2) *we have*

$$\delta((e_u)) \ll p^{3/2} (\log p)$$

and

$$\gamma_\ell((e_u)) \ll \ell p^{5/3}.$$

Proof. Note that for $0 \le c < m$ and $q_p(u) \not\equiv 0 \bmod p$,

$$\frac{1}{m} \sum_{j=0}^{m-1} (\chi(q_p(u)) \exp(-2\pi i c/m))^j = \begin{cases} 1, & \text{if } e_u = c, \\ 0, & \text{otherwise,} \end{cases}$$

and thus

$$x((e_u), c, M, a, b) \ll \frac{1}{m} \sum_{u=0}^{M-1} \sum_{j=0}^{m-1} \chi^j(q_p(au+b)) \exp(-2\pi i c/m))^j + p.$$

The contribution for $j = 0$ is M/m and we get

$$\left| x((e_u), c, M, a, b) - \frac{M}{m} \right| \ll p + \max_{1 \le j < m} \left| \sum_{u=0}^{M-1} \chi^j(q_p(au+b)) \right|.$$

If $a \ge p$, we may assume $M \le p$ and use the trivial bound M for the right hand side. Otherwise we can apply (1) and get the first result.

Similarly we see that

$$\begin{aligned} & \left| g((e_u), w, M, D) - \frac{M}{m^\ell} \right| \\ \ll \; & \ell p + \max_{j_1, \ldots, j_\ell} \left| \sum_{u=0}^{M-1} \chi(q_p(u+d_1)^{j_1} \cdots q_p(u+d_\ell)^{j_\ell}) \right|, \end{aligned}$$

where the maximum is taken over all $0 \le j_1, \ldots, j_\ell \le m-1$ with at least one nonzero j_i. Now the bound follows from Theorem 1. $\square$

For $N \ge 2$ the Nth *linear complexity* $L((e_u), N)$ of (e_u) (modulo m) is the length L of a shortest linear recurrence

$$e_{u+L} \equiv g_{L-1}e_{u+L-1} + \cdots + g_1 e_{u+1} + g_0 e_u \bmod m, \quad u = 0, \ldots, N-L-1, \tag{5}$$

for some integers $g_0, \ldots, g_{L-1}$. For surveys on linear complexity and related measures we refer to [12, 17].

Theorem 3 *For $N \ge 2$ we have*

$$L((e_u), N) \gg \min\left\{\frac{N}{p^{3/2}\log p},\ p^{1/3}\right\}.$$

Proof. Let the first N elements of (e_u) satisfy a linear recurrence (5) of length L. There are at most $\ll Lp$ different $0 \le u \le N-L-1$ with $q_p(u+j) = 0$ for some $0 \le j \le L-1$. For all other u we have

$$1 = \chi\left(q_p(u+L)^{-1}\prod_{l=0}^{L-1} q_p(u+k)^{g_k}\right)$$

and thus

$$\begin{aligned} N &\ll Lp + \sum_{u=0}^{N-L-1} \chi(q_p(u)^{g_0} q_p(u+1)^{g_1} \ldots q_p(u+L)^{p-2}) \\ &\ll \max\left\{\frac{LN}{p^{1/3}}, Lp^{3/2}\log p\right\} \end{aligned}$$

by Theorem 1 and the result follows. $\square$

4 Final remarks

Let (ε_u) be any complex p-periodic sequence. The bounds in (1) and Theorem 1 can be easily extended to

$$\sum_{u=0}^{N-1} \psi(q_p(au+b))\varepsilon_u \ll \sum_{u=0}^{p-1} |\varepsilon_u| N^{1-\nu}(N/p)^{(\nu+1)/(4\nu^2)}(\log p)^{1/\nu}$$

and

$$\begin{aligned}&\sum_{u=0}^{N-1} \psi_1(q_p(u+d_1))\cdots\psi_\ell(q_p(u+d_\ell))\varepsilon_u\\ \ll\ &\max\{\max_{0\le u<p}|\varepsilon_u|\ell N p^{-1/3}, \sum_{u=0}^{p-1}|\varepsilon_u|\ell p^{1/2}\log p\}.\end{aligned}$$

Hence, the bounds of Theorems 2 and 3 are valid for the more general sequences $(e_u + c_u)$ for any p-periodic sequence (c_u) over $\{0, 1, \ldots, m-1\}$.

Another definition of the correlation measure, which coincides with the definition for binary sequences [10], was also introduced in [11].

Let $\mathcal{E}_m = \{\varepsilon_1, \ldots, \varepsilon_m\}$ be the set of the complex m-th roots of unity, and let $\mathcal{F}$ be the set of $m!$ bijections φ of $\mathcal{E}_m$. For $\phi = (\varphi_1, \ldots, \varphi_\ell) \in \mathcal{F}^\ell$ and $D = (d_1, \ldots, d_\ell)$ with non-negative integers $0 \le d_1 < \cdots < d_\ell$ write

$$G((e_u), \phi, M, D) = \sum_{u=0}^{M-1} \varphi_1(\exp(2\pi i e_{u+d_1}/m))\cdots\varphi_\ell(\exp(2\pi i e_{u+d_\ell}/m)).$$

Then the *$\mathcal{E}_m$-correlation measure of order ℓ* of (e_u) is defined as

$$\Gamma_\ell((e_u)) = \max_{\phi,M,D} |G((e_u), \phi, M, D)|,$$

where the maximum is taken over all $\phi \in \mathcal{F}^\ell$, and $D = (d_1, \ldots, d_\ell)$ with non-negative integers $0 \le d_1 < \ldots < d_\ell$ and M such that $M + d_\ell \le p^2$. The connection between the f-correlation measure and the $\mathcal{E}_m$-correlation measure was investigated in [11]. They are 'nearly equivalent' by the following relation

$$\frac{1}{m^\ell}\Gamma_\ell((e_u)) \le \gamma_\ell((e_u)) \le \sum_{t=1}^{\ell} \left(\begin{array}{c} \ell \\ t \end{array} \right) (m-1)^t \Gamma_\ell((e_u)).$$

The relations between the correlation measures of order ℓ and the Nth linear complexity of [2, 4] can be used to obtain bounds on the Nth linear complexity of (e_u) as well. However, the direct use of the character sum bound in Theorem 1 gives a better nontrivial bound if $p^{3/2}\log p \le N \le p^{11/6}\log p$.

In [11] the (p-periodic) sequence (e'_u) of *discrete logarithms modulo m* of u (instead of $q_p(u)$ in this paper) was studied and the bound (Theorem 3)

$$\gamma_\ell((e'_u)) \ll m\ell p^{1/2}\log p$$

proved. However, the m can be omitted since Weil's bound on complete character sums and thus the bound on the incomplete sums

$$\sum_{u=0}^{M-1} \chi(f(u))$$

doesn't depend on the degree of $f(X)$ (here $\leq m\ell$) but only on its number of different zeros (here $\leq \ell$), see for example [14, Lemma 3.4].

References

[1] Aly, H., Winterhof, A.: Boolean functions derived from Fermat quotients, Preprint (2010).

[2] Brandstätter, N., Winterhof, A.: Linear complexity profile of binary sequences with small correlation measure, Period. Math. Hungar. 52 (2006), 1–8.

[3] Chen Z., Ostafe, A., Winterhof. A.: Structure of pseudorandom numbers derived from Fermat quotients. in WAIFI 2010, Lecture Notes in Comput. Sci. 6087 (2010), 73–85.

[4] Chen, Z., Winterhof, A.: Linear complexity profile of m-ary pseudorandom sequences with small correlation measure, Indag. Math. 20 (2009), 631–640.

[5] Chen, Z., Winterhof, A.: On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients, Int. J. Number Theory. 8 (2012), 631–641.

[6] Ernvall, R., Metsänkylä, T.: On the p-divisibility of Fermat quotients, Math. Comp. 66 (1997), 1353–1365.

[7] Granville, A.: Some conjectures related to Fermat's Last Theorem, In Number Theory (Banff, 1988) de Gruyter, NY, 1990, 177–192.

[8] Heath-Brown, R.: An estimate for Heilbronn's exponential sum, In Analytic Number Theory, Vol. 2, Progr. Math. 139 (1996), 451–463.

[9] Iwaniec, H., Kowalski, E.: Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[10] Mauduit, C., Sárközy, A.: On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol, Acta Arith. 82 (1997), 365–377.

[11] Mauduit C., Sárközy A.: On finite pseudorandom sequences of k symbols, Indag. Math. (N.S.) 13 (2002), 89–101.

[12] Niederreiter, H.: Linear complexity and related complexity measures for sequences. In *Progress in Cryptology—INDOCRYPT 2003. Lecture Notes in Comput. Sci.* 2904 (2003), 1–17.

[13] Ostafe, A., Shparlinski, I. E.: Pseudorandomness and dynamics of Fermat quotients. Preprint (2010).

[14] Shparlinski, I.: Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness. Birkhäuser, 2003.

[15] Shparlinski, I. E.: Character sums with Fermat quotients, Quart. J. Math. Oxford (to appear).

[16] Topuzoğlu, A., Winterhof, A.: Pseudorandom sequences. In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 135–166. Springer, Dordrecht, 2007.

[17] Winterhof, A.: Linear complexity and related complexity measures. In *Selected topics in information and coding theory*, pages 3–40. World Scientific, 2010.